# Maximal $T$-spaces of the free associative algebra over a finite field

C. Bekh-Ochir and S. A. Rankin

January 20, 2013

**Abstract**

In earlier work, it was established that for any finite field $k$, the free associative $k$-algebra on one generator $x$, denoted by $k[x]_0$, had infinitely many maximal $T$-spaces, but exactly two maximal $T$-ideals (each of which is a maximal $T$-space). However, aside from these two $T$-ideals, no examples of maximal $T$-spaces of $k[x]_0$ have been identified. This paper presents, for each finite field $k$, an infinite sequence of proper $T$-spaces of $k[x]_0$ (no one of which is a $T$-ideal), each of finite codimension, and for each one, both a linear basis for the $T$-space itself and a linear basis for a complementary linear subspace are provided. Morever, it is proven that the first $T$-space in the sequence is a maximal $T$-space of $k[x]_0$, thereby providing the first example of a maximal $T$-space of $k[x]_0$ that is not a maximal $T$-ideal.

## 1 Introduction

Let $k$ be a field, and let $A$ be an associative $k$-algebra. A. V. Grishin introduced the concept of a $T$-space of $A$ ([3], [4]); namely, a linear subspace of $A$ that is invariant under the natural action of the transformation monoid $T$ of all $k$-algebra endomorphisms of $A$. A $T$-space of $A$ that is also an ideal of $A$ is called a $T$-ideal of $A$. For any $H \subseteq A$, the smallest $T$-space of $A$ containing $H$ shall be denoted by $H^S$, while the smallest $T$-ideal of $A$ that contains $H$ shall be denoted by $H^T$. The set of all $T$-spaces of $A$ forms a lattice under the inclusion ordering.

We shall let $k\langle X\rangle_0$ denote the free associative $k$-algebra on a set $X$. Our interest in this paper shall be the study of the maximal elements in the lattice $L(k\langle X\rangle_0)$ for $X$ any nonempty set. It was shown in [1] that if $k$ is infinite, then the unique maximal $T$-ideal of $k\langle X\rangle_0$ (more precisely, there is a maximum $T$-ideal) is also the unique maximal $T$-space, while the story for $k$ finite was strikingly different. It turned out that when $k$ is finite, there are two maximal $T$-ideals, each of which is a also a maximal $T$-space, but now there are infinitely many maximal $T$-spaces of $k\langle X\rangle_0$. This was established by showing that there is a natural bijection between the sets of maximal $T$-spaces of $k\langle X\rangle_0$ and of $k[x]_0$, and then proving the result for $k[x]_0$.

While the approach taken in [1] treated the cases $p > 2$ and $p = 2$ separately, in each case an infinite family of $T$-spaces was constructed with the property that no maximal $T$-space of $k[x]_0$ could contain more than one of the constructed $T$-spaces. It was not proven in [1] that any of the constructed $T$-spaces was in fact maximal, and it has turned out that the maximal $T$-spaces of $k[x]_0$ (other than the maximum $T$-ideal) are elusive creatures.

Our objective in this paper is to present, for any finite field $k$, another infinite sequence of $T$-spaces of $k[x]_0$ with the hope that each member of the sequence is maximal. Each of these $T$-spaces has finite codimension, and for each of these $T$-spaces, we are able to provide both a linear basis for the $T$-space and a linear basis for a complementary linear subspace of $k[x]_0$. Moreover, we shall prove that the first $T$-space in the sequence is maximal.

Throughout the paper, $k$ shall denote an arbitrary field of order $q$ and characteristic $p \geq 2$.

Let $X$ be any nonempty set. In $k\langle X\rangle_0$, if $|X| = 1$, let $T^{(2)} = \{\, 0 \,\}$, and $Z_X = \{\, x^2 \,\}^T$, where $X = \{\, x \,\}$, otherwise let $x, y \in X$ with $x \neq y$ and set $T^{(2)} = \{\, [x, y] \,\}^T_X$, and $Z_X = \{\, xy \,\}^T$. For any $x \in X$, let $W = T^{(2)} + \{\, x - x^q \,\}^T_X$.

For any finite field $k$, and any nonempty set $X$, $Z$ and $W$ are maximal $T$-ideals of $k\langle X\rangle_0$, and these are the only maximal $T$-ideals of $k\langle X\rangle_0$. It was established in [1] that each is a maximal $T$-space of $k\langle X\rangle_0$. As well, it was established that for $x \in X$, the map $\pi : L(k\langle X\rangle_0) \to L(k[x]_0)$ that is determined by sending each $y \in X$ to $x$ induces a bijection from the set of maximal $T$-spaces of $k\langle X\rangle_0$ onto the set of maximal $T$-spaces of $k[x]_0$. This established that every maximal $T$-space of $k\langle X\rangle_0$ is uniquely determined by its one-variable polynomials.

The following notion will be of fundamental importance in our work. Recall that $k$ is a finite field of order $q$. For monomials $u_i \in k\langle X\rangle_0$ and $\alpha_i \in k$, $1 \leq i \leq t$, $f = \sum_{i=1}^{t} \alpha_i u_i$ shall be said to be $q$-homogeneous if for each $x \in X$ and each $i, j$ with $1 \leq i, j \leq t$, $\deg_x(u_i) \equiv \deg_x(u_j) \pmod{q-1}$.

## 2 A sequence $W_n$, $n \geq 1$, of $T$-spaces of $k\langle X\rangle_0$

**Definition 2.1.** *Let $X$ be a nonempty set, and let $x \in X$. For each $n \geq 1$, let $W_n(X)$ denote the $T$-space of $k\langle X\rangle_0$ that is generated by $x + x^{q^n}$ and $x^{q^n+1}$; that is, $W_n(X) = \{\, x + x^{q^n} \,\}^S + \{\, x^{q^n+1} \,\}^S$. As well, let $U_n(X) = \{\, x - x^{q^{2n}} \,\}^T$ in $k\langle X\rangle_0$. If $X$ is finite, say $X = \{\, x_1, x_2, \ldots, x_m \,\}$, we shall write $W_n(x_1, x_2, \ldots, x_m)$ and $U_n(x_1, x_2, \ldots, x_m)$ for $W_n(X)$ and $U_n(X)$, respectively. Finally, if $X = \{\, x \,\}$, we shall simply write $W_n$ and $U_n$ for $W_n(X)$ and $U_n(X)$, respectively.*

There is a very important observation that we may make about $U_n$ that will have interesting applications in the work to come.

**Lemma 2.1.** *Let $x \in X$. Then for any $u \in k[x]_0 \subseteq k\langle X\rangle_0$, $x^{q^{2n}-1}u \equiv u \ (mod\, U_n)$.*

*Proof.* It suffices to prove the result for $u = x^i$, $i \geq 1$. If $i = 1$, the result follows from the definition of $U_n$. Suppose that $i \geq 2$. Then $x^{q^{2n}-1}x^i = x^{q^{2n}}x^{i-1} \equiv xx^{i-1} = x^i \pmod{U_n}$. $\square$

**Lemma 2.2.** *Let $n \geq 1$. Then for any $u, v \in k\langle X\rangle_0$, $uv^{q^n} + u^{q^n}v \in W_n(X)$.*

*Proof.* For any $u, v \in k\langle X\rangle_0$, we have $(u+v)^{q^n+1} = (u+v)^{q^n}(u+v) = (u^{q^n} + v^{q^n})(u+v) = u^{q^n+1} + u^{q^n}v + v^{q^n}u + (uv)^{q^n}$. Since $(u+v)^{q^n+1}$, $u^{q^n+1}$, and $v^{q^n+1}$ each belong to $W_n(X)$, it follows that $u^{q^n}v + v^{q^n}u \in W_n(X)$. $\square$

**Lemma 2.3.** *For every $n \geq 1$, $U_n(X) \subseteq W_n(X)$.*

*Proof.* Let $u, v \in k\langle X\rangle_0$. Then $(u+u^{q^n})(v+v^{q^n}) = uv + uv^{q^n} + u^{q^n}v + (uv)^{q^n}$. As $uv + (uv)^{q^n} \in W_n(X)$ by definition, and by Lemma 2.2, $uv^{q^n} + u^{q^n}v \in W_n(X)$, it follows that $(u+u^{q^n})(v+v^{q^n}) \in W_n(X)$. Now note that $(u - u^{q^{2n}})(v+v^{q^n}) = (u+u^{q^n})(v+v^{q^n}) - (u^{q^n} + (u^{q^n})^{q^n})(v+v^{q^n})$, and thus, since $(u+u^{q^n})(v+v^{q^n}) \in W_n(X)$, and $(u^{q^n} + (u^{q^n})^{q^n})(v+v^{q^n}) \in W_n(X)$, we have $(u - u^{q^{2n}})(v+v^{q^n}) \in W_n(X)$. But

$$\begin{aligned}(u - u^{q^{2n}})(v+v^{q^n}) &= (u - u^{q^{2n}})v + uv^{q^n} - u^{q^{2n}}v^{q^{2n}} \\ &= (u - u^{q^{2n}})v + uv^{q^n} + u^{q^n}v - (u^{q^n}v + (u^{q^n}v)^{q^n}).\end{aligned}$$

By Lemma 2.2, $uv^{q^n} + u^{q^n}v \in W_n(X)$, and by definition, $u^{q^n}v + (u^{q^n}v)^{q^n} \in W_n(X)$. As well, we have shown that $(u - u^{q^{2n}})(v+v^{q^n}) \in W_n(X)$, and so it follows that $(x - x^{q^{2n}})v \in W_n(X)$. $\square$

In the proof of the preceding lemma, we showed that $(u+u^{q^n})(v+v^{q^n}) \in W_n(X)$ for every $u, v \in k\langle X\rangle_0$. We can say more in this regard. For any $u, v \in k\langle X\rangle_0$, we have

$$(u+u^q)v^{q^n+1} = uv^{q^n+1} + u^{q^n}v^{q^n+1} \equiv uv^{q^n+1} - u(v^{q^n+1})^{q^n} \pmod{W_n(X)}.$$

As well, $u(v^{q^n+1})^{q^n} = uv^{q^{2n}+q^n} \equiv uv^{1+q^n} \pmod{U_n(X)}$. Since $U_n(X) \subseteq W_n(X)$, we have $(u+u^q)v^{q^n+1} \equiv uv^{q^n+1} - uv^{q^n+1} = 0 \pmod{W_n(X)}$, so $(u+u^q)v^{q^n+1} \in W_n(X)$. A similar argument shows that $v^{q^n+1}(u+u^q) \in W_n(X)$. Thus for each $n \geq 1$, $W_n(X)$ is a subalgebra of $k\langle X\rangle_0$.

We now explore more carefully the case when $X = \{ x \}$, in which case $k\langle X\rangle_0 = k[x]_0$.

**Lemma 2.4.** *The set $\{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$ is a linear basis for $U_n$.*

*Proof.* For any $\alpha, \beta \in k$ and $v, w \in k[x]_0$, $(\alpha v + \beta w)^{q^{2n}} - (\alpha v + \beta w) = \alpha v^{q^{2n}} + \beta w^{q^{2n}} - \alpha v - \beta w = \alpha(v^{q^{2n}} - v) + \beta(w^{q^{2n}} - w)$. Consider $u \in U_n$. We have $u = \sum_{i=1}^t \alpha_i(u_i^{q^{2n}} - u_i)v_i$ for some $u_1, v_1, u_2, v_2, \ldots, u_t, v_t \in k[x]_0$ and $\alpha_1, \ldots, \alpha_t \in k$. By the above observation, we may assume that each $u_i$ is a monomial; that is, we may assume that $u$ has the form $u = \sum_{i=1}^t \alpha_i((x^{r_i})^{q^{2n}} - x^{r_i})v_i$ for positive integers $r_i$, $i = 1, \ldots, t$. For each $i$, by factoring as a difference of $r_i$ powers,

we may write $(x^{r_i})^{q^{2n}} - x^{r_i} = (x^{q^{2n}} - x)w_i$, for some $w_i \in k[x]_0$. For each $i$, $(x^{q^{2n}} - x)w_i v_i$ is in the linear space spanned by $\{ (x^{q^{2n}} - x)x^j \mid j \geq 0 \}$. Since $x^{q^{2n}} - x \in U_n$, we have $(x^{q^{2n}} - x)x^j \in U_n$ for each $j \geq 1$, and so it follows that the set $\{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$ is a spanning set for $U_n$. The linear independence is immediate since no two polynomials in the set have the same degree. $\square$

The set $\{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$ contains exactly one polynomial of each degree greater than or equal to $q^{2n}$, and so the dimension of $k[x]_0/U_n$ as a $k$-vector space is $q^{2n} - 1$. Note that if $1 \leq m \leq q^{2n} - 1$, then by the division theorem, there exist unique integers $t$ and $r$ with $m = tq^n + r$ and $0 \leq r < q^n$. Since $n \leq q^{2n} - 1$, we have $tq^n + r \leq q^{2n} - 1$, so $t \leq q^n - (r+1)/q^n \leq q^n - 1/q^n$. Since $t$ is an integer, it follows that $t \leq q^n - 1$, so we have $0 \leq t, r \leq q^b - 1$ and not both $t$ and $r$ can be 0. The uniqueness of $t$ and $r$ establishes that no two polynomials in the set

$$\{ x^{q^n i + j} + x^{i + q^n j} \mid q^n > i > j \geq 0 \} \cup \{ (x^{q^n + 1})^i \mid 1 \leq i \leq q^n - 1 \}$$

have the same degree, which establishes the following fact.

**Lemma 2.5.** *The set*

$$\{ x^{q^n i + j} + x^{i + q^n j} \mid q^n > i > j \geq 0 \} \cup \{ (x^{q^n + 1})^i \mid 1 \leq i \leq q^n - 1 \}$$

*is linearly independent in $k[x]_0$.*

**Definition 2.2.** *For each $n \geq 1$, and $i, j$ with $0 \leq i, j < q^n$ and $i \neq j$, let $F(i,j) = x^{iq^n + j} + x^{i + jq^n}$, and let $F(i,i) = (x^{q^n+1})^i$ if $1 \leq i < q^n$. Then set*

$$E_n = \{ F(i,j) \mid q^n > i > j \geq 0 \} \cup \{ F(i,i) \mid 1 \leq i \leq q^n - 1 \},$$

*and let $V_n$ denote the linear span of $E_n$ in $k[x]_0$.*

It follows from Lemma 2.5 that the dimension of $V_n$ (as a $k$-vector space) is $\binom{q^n}{2} + q^n - 1$. Furthermore, we note that if $0 \leq j < i < q^n$, then the degree of $F(i,j) = F(j,i)$ is $iq^n + j$.

Note that if $p > 2$, the set $\{ x^{q^n i + j} + x^{i + q^n j} \mid q^n > i \geq j \geq 0,\ i + j > 0 \}$ is a basis for $V_n$, as taking $i = j$ in $x^{q^n i + j} + x^{i + q^n j}$ gives $2(x^{q^n + 1})^i$.

**Proposition 2.1.** *For each $n \geq 1$, $W_n = V_n \oplus U_n$.*

*Proof.* Note that when $i > j = 0$, then $x^{q^n i + j} + x^{i + q^n j} = x^{q^n i} + x^i \in W_n$, while if $i > j > 0$, $x^{q^n i + j} + x^{i + q^n j} \in W_n$ by virtue of Lemma 2.2. Thus $V_n \subseteq W_n$. Furthermore, as the elements of $E_n$ have degree at most $q^n(q^n - 1) + q^n - 1 = q^{2n} - 1 < q^{2n}$, no two elements of $E_n \cup \{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$ have the same degree, so $E_n \cup \{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$ is linearly independent and $V_n \cap U_n = \{ 0 \}$. It remains to prove that $E_n \cup \{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$ is a spanning set for $W_n$.

Observe that $(u+v)^{q^n+1} = u^{q^n+1} + v^{q^n+1} + (uv^{q^n} + u^{q^n}v)$, and the expression $(uv^{q^n} + u^{q^n}v)$ is linear in each of $u$ and $v$, so the set $\{ F(i,j) \mid i > j \geq 1 \} \cup$

$\{ F(i,i) \mid i \geq 1 \}$ is a basis for $\{ x^{q^n+1} \}^S$, while the set $\{ F(i,0) \mid i > 0 \}$ is a basis for $\{ x + x^{q^n} \}^S$. Thus the set $\{ F(i,j) \mid i \geq j,\ i+j \neq 0 \}$ is a linear basis for $W_n$. It suffices therefore to prove that for each $i > 0$, there exists $i_1$ with $q^n > i_1 \geq 1$ such that $F(i,i) \equiv F(i_1,i_1) \pmod{U_n}$, and for each $j$ with $i > j \geq 0$, there exist $i_1, j_1$ with $q^n > i_1 \geq j_1 \geq 0$ and $i_1 + j_1 > 0$ such that $F(i,j) \equiv F(i_1,j_1) \pmod{U_n}$. This we do by induction on $i \geq 1$. The assertion is obviously true for $1 \leq i \leq q^n - 1$, so we suppose that $i \geq q^n$ is such that the assertion holds for all smaller integers. Let $t = i - q^n \geq 0$. Then $F(i,i) = (x^{q^n+1})^i = (x^{q^n+1})^{(t+q^n)} = x^{q^{2n}+q^n t+t+q^n} \equiv x^{1+q^n t+t+q^n} = F(t+1,t+1) \pmod{U_n}$, and $t+1 < t+q^n = i$, so by the induction hypothesis, there exists $i_1 < q^n$ such that $F(t+1,t+1) \equiv F(i_1,i_1) \pmod{U_n}$. But then $F(i,i) \equiv F(t+1,t+1) \equiv F(i_1,i_1) \pmod{U_n}$, as required. Now let $0 \leq j < i$. Suppose first that $j \geq q^n$ as well. For $i = t + q^n$ and $j = r + q^n$, we have $F(i,j) = x^{(t+q^n)q^n+r+q^n} + x^{t+q^n+(r+q^n)q^n} = x^{tq^n+q^{2n}+r+q^n} + x^{t+q^n+rq^n+q^{2n}} \equiv x^{tq^n+1+r+q^n} + x^{t+q^n+rq^n+1} = F(t+1,r+1)$. By the induction hypothesis, since $i > t+1 > r+1 \geq 0$, there exist $i_1, j_1$ with $q^n > i_1 \geq j_1 \geq 0$ and $i_1 + j_1 > 0$ such that $F(i,j) \equiv F(i_1,j_1) \equiv F(t+1,r+1) \pmod{U_n}$, as required. Suppose now that $j < q^n$. As before, set $i = t + q^n$, and consider $F(i,j)$. We have $F(i,j) = x^{(t+q^n)q^n+j} + x^{t+q^n+jq^n} = x^{tq^n+q^{2n}+j} + x^{t+q^n+jq^n} \equiv x^{tq^n+1+j} + x^{t+q^n(j+1)} = F(t,j+1) \pmod{U_n}$. Since $i > t$, the result follows from the inductive hypothesis if $t \geq j+1$, or if $t < j+1 < i$. Suppose that $t < j+1 = i$. Since $j < q^n$ and $i \geq q^n$, we must have $i = q^n$ and $j = q^n - 1$. But then $t = 0$, and $F(t,j+1) = F(0,q^n) = x^{q^n} + x^{q^{2n}} \equiv x^{q^n} + x = F(0,1) \pmod{U_n}$, which completes the proof of the inductive step. Thus $E_n \cup \{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$ is a spanning set for $W_n$. $\square$

We remark that in the proof of Proposition 2.1, it was established that

$$E_n \cup \{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$$

is a linear basis for $W_n$.

**Corollary 2.1.** $\dim(k[x]_0/W_n) = \binom{q^n}{2}$. *In particular, $W_n$ is a proper $T$-space of $k[x]_0$.*

*Proof.* The dimension of $k[x]_0/W_n$ is $q^{2n} - 1 - (q^n(q^n-1)/2 + q^n - 1) = q^{2n}/2 - q^n/2 = q^n(q^n-1)/2 = \binom{q^n}{2}$. $\square$

# 3 The maximality of $W_n$

In this section, we begin to investigate the maximality of $W_n$ in $k[x]_0$ for $n \geq 1$.

We have seen that each integer $m$ with $1 \leq m \leq q^{2n} - 1$ is uniquely of the form $m = tq^n + r$ with $0 \leq t, r < q^n$ and $t + r > 0$. Thus in the set $E_n \cup \{ (x^{q^{2n}} - x)x^i \mid i \geq 0 \}$, there are no polynomials with degree of the form $jq^n + i$ with $q^n > i > j \geq 0$. Consequently,

$$E_n \cup \{ (x^{q^2 n} - x)x^i \mid i \geq 0 \} \cup \{ x^{i+q^n j} \mid q^n > i > j \geq 0 \}$$

is linearly independent in $k[x]_0$, and contains polynomials of each degree greater than or equal to 1, hence is a linear basis for $k[x]_0$. It follows that the set $\{ x^{i+q^n j} \mid q^n > i > j \geq 0 \}$ containing $\binom{q^n}{2}$ polynomials is a $k$-linear basis for a subspace of $k[x]_0$ that is complentary to $W_n$.

**Definition 3.1.** *For each $n \geq 1$, let $B_n = \{ x^{i+q^n j} \mid q^n > i > j \geq 0 \}$, and let $Y_n$ denote the linear subspace of $k[x]_0$ that is spanned by $B_n$.*

Thus $k[x]_0 = Y_n \oplus W_n = Y_n \oplus V_n \oplus U_n$. In order to establish that $W_n$ is maximal, it suffices to show that for any nonzero $f \in Y_n$, $W_n + \{ f \}^S = k[x]_0$. Moreover, since each $q$-homogeneous component of $f$ belongs to any $T$-space that contains $f$, it will suffice to prove that for any nonzero $q$-homogeneous polynomial $f \in Y_n$, $W_n + \{ f \}^S = k[x]_0$.

**Lemma 3.1.** *For any positive integer $r$, the following hold in $k[x]_0$.*

*(i)* $x^{q^{2^r m}} \equiv x^{q^{2^r (m-2)}} \pmod{U_{2^r}}$ *for any $m \geq 3$.*

*(ii)* $x + (-1)^{m+1} x^{q^{2^r m}} \in \{ x + x^{q^{2^r}} \}^S$ *for any $m \geq 1$.*

*Proof.* Let $m \geq 3$. We have $q^{2^r m} = q^{2^r (m-2) + 2^{r+1}} = q^{2^r (m-2)} q^{2^{r+1}}$, and so

$$x^{q^{2^r m}} = (x^{2^{r+1}})^{q^{2^r (m-2)}} \equiv x^{q^{2^r (m-2)}} \pmod{U_{2^r}},$$

which establishes the first part. The second part is proven by induction on $m \geq 1$, with the case for $m = 1$ true by definition. Suppose that $m \geq 1$ is an integer for which the result holds, so $x + (-1)^{m+1} x^{q^{2^r m}} \in \{ x + x^{q^{2^r}} \}^S$. Apply the substitution $x \mapsto x^{q^{2^r m}}$ to $x + x^{q^{2^r}}$ to obtain that $x^{q^{2^r m}} + x^{q^{2^r m} q^{2^r}} \in \{ x + x^{q^{2^r}} \}^S$. Thus $x + (-1)^{m+2} x^{q^{2^r (m+1)}} = x + (-1)^{m+1} x^{q^{2^r m}} + (-1)^{m+2} [x^{q^{2^r m}} + x^{q^{2^r (m+1)}}] \in \{ x + x^{q^{2^r}} \}^S$. The result follows now by induction. □

**Proposition 3.1.** *For each $r \geq 1$ and each odd $m \geq 1$, $W_{2^r m} \subseteq W_{2^r}$.*

*Proof.* By Lemma 3.1 (i) and induction on odd $m \geq 1$, $x^{q^{2^r m}} \equiv x^{q^{2^r}} \pmod{U_{2^r}}$ for every odd $m \geq 1$. Let $m \geq 1$ be odd. Then $x^{q^{2^r m}+1} \equiv x^{q^{2^r}+1} \pmod{U_{2^r}}$. Since $x^{q^{2^r}+1} \in W_{2^r}$ and $U_{2^r} \subseteq W_{2^r}$, it follows that $x^{q^{2^r m}+1} \in W_{2^r}$. Next, since $m$ is odd, it follows from Lemma 3.1 (ii) that $x + x^{q^{2^r m}} \in \{ x + x^{q^{2^r}} \}^S \subseteq W_{2^r}$. Thus $W_{2^r m} = \{ x + x^{q^{2^r m}} \}^S + \{ x^{q^{2^r m}+1} \}^S \subseteq \{ x + x^{q^{2^r}} \}^S + \{ x^{q^{2^r}+1} \}^S = W_{2^r}$. □

The next question is whether or not $W_{2^s} \subseteq W_{2^r}$ when $s \geq r$. It follows from the next result that this is never the case.

**Proposition 3.2.** *Let $s > r \geq 0$ be integers. Then $W_{2^r} + W_{2^s} = k[x]_0$.*

*Proof.* Let $V = W_{2^r} + W_{2^s}$. By Lemma 3.1 (i), if we let $s = r + t$ with $t \geq 1$, we have $x^{q^{2^s}} = x^{q^{2^r 2^t}} \equiv x^{q^{2^r 2}} = x^{q^{2^{r+1}}} \equiv x \pmod{U_{2^r}}$, and so $x^{q^{2^s}+1} \equiv$

$x^2 \pmod{U_{2^r}}$. But then $x^2 \in V$. Consider first the case when $p > 2$. From $(x + x^{q-1})^2 - x^2 - (x^{q-1})^2 \in V$, we obtain that $2x^q \in V$ and since $p > 2$, we obtain $x^q \in V$. On the other hand, when $p = 2$, we observe that since $q = 2^t$ for some $t \geq 1$, we again obtain that $x^q \in V$. So in either case, $x^q \in V$, and thus $x^{q^{2^r}} \in V$. Since $x + x^{q^{2^r}} \in V$, we finally obtain $x \in V$, as required. □

Since for any $n \geq 1$, $W_n$ is a proper subspace of $k[x]_0$, it follows immediately that for any $r, s \geq 1$ with $r \neq s$, neither of $W_{2^r}$ and $W_{2^s}$ contains the other, and more generally, no maximal $T$-space of $k[x]_0$ contains both $W_{2^r}$ and $W_{2^s}$.

From here on, $n$ shall denote a power of 2. We wish to show that for any nonzero $f \in Y_n$, $W_n + \{ f \}^S = k[x]_0$. In fact, it suffices to consider only linear combinations of $q$-homogeneous elements of $B_n$; that is, it suffices to prove that if $f$ is any nonzero $q$-homogeneous element of $Y_n$, then $W_1 + \{ f \}^S = k[x]_0$.

# 4 The maximality of $W_1$ in $k[x]_0$

Our objective in this section is to establish that $W_1$ is a maximal $T$-space of $k[x]_0$.

Suppose that $X$ and $Y$ are nonempty sets with $X \subseteq Y$. We shall have occasion to compare the $T$-space of $k\langle X\rangle_0$ (respectively $k[X]_0$) that is generated by a subset $U$ of $k\langle X\rangle_0$ ($k[X]_0$) to the $T$-space of $k\langle Y\rangle_0$ ($k[Y]_0$) that is generated by the same set $U$. When necessary for clarity, for $U \subseteq k\langle X\rangle_0$ ($k[X]_0$), we shall write $U_X^S$, rather than $U^S$, to denote the $T$-space of $k\langle X\rangle_0$ ($k[X]_0$) that is generated by $U$. Accordingly, $U_Y^S$ would denote the $T$-space of $k\langle Y\rangle_0$ ($k[Y]_0$) generated by $U$.

**Proposition 4.1.** *Let $X$ and $Y$ be nonempty sets with $X \subseteq Y$.*

*(i) For any $U \subseteq k\langle X\rangle_0$, $U_X^S = U_Y^S \cap k\langle X\rangle_0$.*

*(ii) For any $U \subseteq k[X]_0$, $U_X^S = U_Y^S \cap k[X]_0$.*

*Proof.* We shall prove the first part; the proof of the second is similar and will be omitted. Since every algebra endomorphism of $k\langle X\rangle_0$ extends to an algebra endomorphism of $k\langle Y\rangle_0$, it follows that $U_X^S \subseteq U_Y^S$, and thus $U_X^S \subseteq U_Y^S \cap k\langle X\rangle_0$. It remains to prove that $U_Y^S \cap k\langle X\rangle_0 \subseteq U_X^S$. Let $u \in U_Y^S \cap k\langle X\rangle_0$. Then there exist $\alpha_i \in k$, $f_i\colon k\langle Y\rangle_0 \to k\langle Y\rangle_0$, $u_i \in U$, with $u = \sum \alpha_i f_i(u_i)$. Let $g\colon k\langle Y\rangle_0 \to k\langle Y\rangle_0$ be the map determined by $x \mapsto x$ if $x \in X$, while $x \mapsto 0$ if $x \in Y - X$. As well, let $\iota\colon k\langle X\rangle_0 \to k\langle Y\rangle_0$ be the map determined by $\iota(x) = x$ for each $x \in X$. Then since $u \in k\langle X\rangle_0$, we have $u = g(u) = \sum \alpha_i g \circ f_i(u_i)$, and since $u_i \in U$, we have $u_i = \iota(u_i)$, so $u = \sum \alpha_i g \circ f_i \circ \iota(u_i)$. Since $g \circ f_i \circ \iota\colon k\langle X\rangle_0 \to k\langle X\rangle_0$, and $u_i \in U$ for each $i$, it follows that $u \in U$. □

For $x \in X$, we shall make use of the homomorphism $\pi\colon k\langle X\rangle_0 \to k[x]_0$ that is determined by sending each $z \in X$ to $x$. For each $T$-space $V$ of $k\langle X\rangle_0$, $\pi V = V \cap k[x]_0$, where we regard $k\langle X\rangle_0$ as a subalgebra of $k\langle X\rangle_0$ in the natural way. This follows from the fact that $V$ is a $T$-space, and we can consider $\pi$

as an endomorphism of $k\langle X\rangle_0$, so $\pi(V) \subseteq V$. Thus $\pi(V) \subseteq V \cap k[x]_0$. For $f \in V \cap k[x]_0$, $\pi(f) = f$ and so $f \in \pi(V)$, which proves that $V \cap k[x]_0 \subseteq \pi(V)$.

**Lemma 4.1.** *Let $X$ be any set of size at least two, and let $x \in X$. For any $U \subseteq k[x]_0$ and $f \in k[x]_0$, $f \in U^S$ if and only if $f \in U^{S_X} + T^{(2)}$, where $T^{(2)}$ is the commutator $T$-ideal of $k\langle X\rangle_0$ (so generated by $[x, y]$ for any $y \in X$).*

*Proof.* Since $T^{(2)} \subseteq \ker(\pi)$, we have $\pi(U^{S_X} + T^{(2)}) = \pi(U^{S_X}) = U^{S_X} \cap k[x]_0$, and by Proposition 4.1, $U^{S_X} \cap k[x]_0 = U^S$. For $f \in k[x]_0$, we have $\pi(f) = f$, so $f \in U^{S_X} + T^{(2)}$ implies that $f = \pi(f) \in U^S$, while the converse follows from the fact that $U^S \subseteq U^{S_X} \subseteq U^{S_X} + T^{(2)}$. □

**Corollary 4.1.** *Let $X$ be any set of size at least two, and let $x \in X$. For any $U \subseteq k[x]_0$ and $f \in k[x]_0$, $f \in U^S$ if and only if $f \in U^{S_X}$ in $k[X]_0$.*

The following result will be very important in our work.

**Proposition 4.2** ([2], Theorem 1)**.** *Let $p$ be a prime, and let*

$$M = M_0 + M_1p + M_2p^2 + \cdots + M_tp^t \qquad (0 \le M_r < p),$$
$$N = N_0 + N_1p + N_2p^2 + \cdots + N_tp^t \qquad (0 \le N_r < p).$$

*Then*

$$\binom{M}{N} \equiv \binom{M_0}{N_0}\binom{M_1}{N_1}\binom{M_2}{N_2}\cdots\binom{M_t}{N_t} \ (mod\, p).$$

We state an immediate consequence of Proposition 4.2 which will be of great value in what follows. Recall that $k$ is a finite field of order $q$ and characteristic $p$, so $q$ is a $p$-power.

**Corollary 4.2.** *For any integers $t, r, i, j$ with $0 \le t, r, i, j < q$,*

$$\binom{tq + r}{jq + i} \equiv \binom{t}{j}\binom{r}{i} \ (mod\, p).$$

**Corollary 4.3.** *Let $j$ and $t$ be integers with $0 \le j \le t$. Then the following hold:*

*(i) If $1 \le r \le q - 1$ and $t \le r/2$, then modulo $p$,*

$$\binom{r + t(q-1)}{1 + j(q-1)} \equiv \begin{cases} 0 & j > 1 \\ t & j = 1 \\ r - t & j = 0 \end{cases}$$

*(ii) If $1 \le r \le q - 1$ and $r + 1 \le t < (q + r + 1)/2$, then modulo $p$,*

$$choice r + t(q-1), 1 + j(q-1) \equiv \begin{cases} \binom{t-1}{j-1}\binom{q+r-t}{q+1-j} & j > 1 \\ t - 1 & j = 1 \\ r - t & j = 0 \end{cases}$$

*In particular, if $1 < j < t - (r - 1)$, then $\binom{r+t(q-1)}{1+j(q-1)} \equiv 0 \ (mod\, p)$.*

*(iii) If $2 \le r \le q-1$ and $t < r/2$, then modulo $p$,*

$$\binom{r+t(q-1)}{r-1+j(q-1)} \equiv \begin{cases} 0 & j < t-1 \\ t & j = t-1 \\ r-t & j = t \end{cases}$$

*(iv) If $2 \le r \le q-1$ and $r+1 \le t < (q+r+1)/2$, then modulo $p$,*

$$\binom{r+t(q-1)}{r-1+j(q-1)} \equiv \begin{cases} \binom{t-1}{j}\binom{q+r-t}{r-1-j} & j \le r-1 < t-1 \\ 0 & r-1 < j < t-1 \\ t-1 & j = t-1 \\ r-t & j = t \end{cases}$$

*Proof.* For the first part, we observe that $r+t(q-1) = tq + (r-t)$ with $0 \le t, r-t < q$, and $1 + j(q-1) = (j-1)q + (q+1-j) = jq + 1 - j$. If $j > 1$, then $0 \le j-1, q+1-j < q$, while if $j = 0, 1$, then $0 \le j, 1-j < q$. By Corollary 4.2, in the first case we have $\binom{r+t(q-1)}{1+j(q-1)} \equiv \binom{t}{j-1}\binom{r-t}{q+1-j} \pmod p$, while in the second case, we have $\binom{r+t(q-1)}{1+j(q-1)} \equiv \binom{t}{j}\binom{r-t}{1-j} \pmod p$. Note that $q+1-j > r-t$ if and only if $q+1+t-j > r$, which holds since $r \le q-1 < q+1$. Thus when $j > 1$, $\binom{r-t}{q+1-j} \equiv 0 \pmod p$, and so $\binom{r+t(q-1)}{1+j(q-1)} \equiv 0 \pmod p$.

For the second part, we observe that since $r+1 \le t < (q+r+1)/2$, $0 \le t-1 < q+r-t \le q-1$, and so $r+t(q-1) = (t-1)q + (q+r-t)$ with $0 \le t-1, q+r-t < q$. As well, $1+j(q-1) = (j-1)q + (q+1-j) = jq+1-j$, so if $j > 1$, then $0 \le j-1, q+1-j < q$, while if $j = 0, 1$, we have $0 \le j, 1-j < q$. In the first case, we obtain $\binom{r+t(q-1)}{1+j(q-1)} \equiv \binom{t-1}{j-1}\binom{q+r-t}{q+1-j} \pmod p$, while in the second case, we have $\binom{r+t(q-1)}{1+j(q-1)} \equiv \binom{t-1}{j}\binom{q+r-t}{1-j} \pmod p$. Note that if $1 < j < t-(r-1)$, then $q+1-j > q+r-t$ and so $\binom{q+r-t}{q+1-j} \equiv 0 \pmod p$, which establishes that $\binom{r+t(q-1)}{1+j(q-1)} \equiv 0 \pmod p$ when $1 < j < t-(r-1)$.

For (iii), we have $r+t(q-1) = tq + r - t$ with $0 \le t, r-t < q$. As well, for $j \le t$, we have $r-1+j(q-1) = jq + r - 1 - j$ with $0 \le j, r-(j+1) < q$ since $t < r/2$ and so $j+1 \le t+1 < r/2 + 1 \le r$. By Corollary 4.2, $\binom{r+t(q-1)}{r-1+j(q-1)} \equiv \binom{t}{j}\binom{r-t}{r-1-j} \pmod p$. Since $j \le t$, we have $r-j \ge r-t$. If $j < t-1$, then $r-j-1 > r-t$ and so $\binom{r-t}{r-1-j} = 0$. If $j = t-1$, then $\binom{t}{j}\binom{r-t}{r-1-j} = t$, and if $j = t$, then $\binom{t}{j}\binom{r-t}{r-1-j} = r-t$.

Finally, for (iv), we have $r+t(q-1) = (t-1)q + q + r - t$ with $0 \le t-1, q+r-t < q$. For $j \le t$, we have $r-1+j(q-1) = jq+r-1-j$ with $0 \le j, r-1-j < q$ if $j+1 \le r$, while if $j+1 > r$, then we have $r-1+j(q-1) = (j-1)q + q + r - 1 - j$ with $0 \le j-1, q+r-1-j < q$. Consider first the situation when $j+1 > r$. In this case, by Corollary 4.2, we have $\binom{r+t(q-1)}{r-1+j(q-1)} \equiv \binom{t-1}{j-1}\binom{q+r-t}{q+r-1-j} \pmod p$. If $j < t-1$, then $q+r-1-j > q+r-t$ and so $\binom{q+r-t}{q+r-1-j} = 0$. If $j = t-1$, then $\binom{t-1}{j-1}\binom{q+r-t}{q+r-1-j} \equiv t-1 \pmod p$, while if $j = t$, then $\binom{t-1}{j-1}\binom{q+r-t}{q+r-1-j} \equiv r-t \pmod p$. Now suppose that $j+1 \le r$. Note

that $r < t$, so this implies that $j < t-1$. Thus $j = t-1$ or $t$ is not possible in this case. By Corollary 4.2, we have $\binom{r+t(q-1)}{r-1+j(q-1)} \equiv \binom{t-1}{j}\binom{q+r-t}{r-1-j} \pmod p$. $\square$

**Definition 4.1.** *For any $r$ with $1 \le r \le q-1$, let $x^{[r]}$ denote the $q$-homogeneity class of $x^r$. Then for each $r$ with $1 \le r \le q-1$, let $B_1^{[r]} = B_1 \cap x^{[r]}$, so $B_1^{[r]} = \{\, x^{jq+i} \mid q > i > j \ge 0,\ jq+i \equiv r \ (mod\, q-1)\,\}$.*

We shall use induction on $r$ to prove that for any $1 \le r \le q-1$, and any nonzero $f \in Y_1 \cap x^{[r]}$, $W_1 + \{\, f\,\}^S = k[x]_0$.

An element of $Y_1 \cap x^{[r]}$ has the form

$$\sum_{\substack{q>i>j\ge 0\\ j+qi\equiv r \pmod{q-1}}} \alpha_{i,j} x^{jq+i},$$

where for each $i$ and $j$, $\alpha_{i,j} \in k$. Note that since $j < i < q$, the maximum value for $jq+i$ is $(q-2)q + (q-1) = q(q-1)-1$, while the minimum value is 1. Furthermore, $jq+i \equiv r \pmod{q-1}$ if and only if $jq+i = r+t(q-1)$ for some integer $t$. Since $1 \le jq+i \le q(q-1)-1$, we would have $1 \le 1+t(q-1) \le q(q-1)-1$, so $0 \le t(q-1) \le q(q-1)-2$, and thus $0 \le t \le q - \frac{2}{q-1}$; that is, $0 \le t \le q-1$. Of the values of $t$ with $0 \le t \le q-1$, we wish to determine those that cause $x^{r+t(q-1)}$ to be an element of $B_1^{[r]}$. Observe that $r+t(q-1) = tq+r-t = (t-1)q+q+r-t$. If $r \ge t$, then $r+t(q-1) = jq+i$ for $j=t$ and $i = r-t$, and we would then require $q > r-t > t \ge 0$. Now, $1 \le r \le q-1$, $t \ge 0$ ensure that $r-t < q$, but $r-t > t$ if and only if $r > 2t$, or $t < r/2$. Thus, of the integers $t$ with $0 \le t \le r$, $x^{r+t(q-1)} \in B_1^{[r]}$ if and only if $0 \le t < r/2$. Consider now the integers $t$ for which $r < t \le q-1$. Then $r+t(q-1) = (t-1)q+q+r-t$ with $t-1 > 0$ and $q+1-(q-1) \le q+r-t < q+t-t = q$, so $r+t(q-1) = jq+i$ for $j = t-1$ and $i = q+r-t$, and we have verified that $q > i$, and $j \ge 0$ (in fact, $j \ge r \ge 1$). We also must have $i > j$, and this holds if and only if $q+r-t > t-1$; that is, if and only if $q+r+1 > 2t$, or $t < (q+r+1)/2$.

We have therefore established the following result.

**Lemma 4.2.** *For each $r$ with $1 \le r \le q-1$,*

$$B_1^{[r]} = \{\, x^{r+t(q-1)} \mid 0 \le t < r/2 \ \text{or}\ r+1 \le t < (q+r+1)/2\,\}.$$

The base case $r = 1$ of our inductive argument is the content of the next lemma.

**Lemma 4.3.** *For nonzero $f \in x^{[1]} \cap Y_1$, $W_1 + \{\, f\,\}^S = k[x]_0$.*

*Proof.* By Lemma 4.2, $B_1^{[1]} = \{\, x^{1+t(q-1)} \mid t = 0 \text{ or } 2 \le t < (q+2)/2\,\}$. Let $f$ be a nonzero element of $x^{[1]} \cap Y_1$. Then there exist $\alpha_t \in k$ such that

$$f = \alpha_0 x + \sum_{2 \le t < (q+2)/2} \alpha_t x^{1+t(q-1)}.$$

By Corollary 4.1, it suffices to prove that $x$ belongs to the $T$-space of $k[x,y]_0$ that is generated by $\{\, x+x^q, x^{q+1}, f \,\}$; that is, that $x$ belongs to the $T$-space of $k[x,y]_0$ that is generated by $W_1(x,y)$ and $f$. For convenience, let us use $W_1$ to refer to either $W_1(x,y)$ or to $W_1(x)$, and let $W_1+\{\, f \,\}^S$ denote both the $T$-space of $k[x,y]_0$ and the $T$-space of $k[x]_0$ that is generated by $\{\, x+x^q, x^{q+1}, f \,\}$. In $k[x,y]_0$, let $g$ denote the $q$-homogeneous component of $xy^{q-1}$ in $f(x+y)-f(x) \in W_1+\{\, f \,\}^S$, so $g \in W_1+\{\, f \,\}^S$ as well. We have

$$\begin{aligned} g &= \alpha_0 x + \sum_{2\le t<(q+2)/2} \alpha_t \Big(\sum_{j=0}^{t} \binom{1+t(q-1)}{1+j(q-1)} x^{1+j(q-1)} y^{(t-j)(q-1)} \\ &\qquad\qquad - \big(\alpha_0 x + \sum_{2\le t<(q+2)/2} \alpha_t x^{1+t(q-1)}\big)\Big) \\ &= \sum_{2\le t<(q+2)/2} \alpha_t \Big(\sum_{j=0}^{t-1} \binom{1+t(q-1)}{1+j(q-1)} x^{1+j(q-1)} y^{(t-j)(q-1)}\Big). \end{aligned}$$

Now apply Corollary 4.3 (ii) with $r=1$ (note that in particular, this gives $\binom{1+t(q-1)}{1+j(q-1)} \equiv 0 \pmod p$ when $1<j<t$) to obtain that

$$\begin{aligned} g &= \sum_{2\le t<(q+2)/2} \alpha_t((1-t)xy^{t(q-1)} + (t-1)x^q y^{(t-1)(q-1)}) \\ &= (xy^{q-1}-x^q) \sum_{2\le t<(q+2)/2} \alpha_t((1-t)y^{(t-1)(q-1)}. \end{aligned}$$

Let $u = \sum_{2\le t\le(q+1)/2} \alpha_t(1-t)y^{(t-1)(q-1)}$, so $(xy^{q-1}-x^q)u = g \in W_1 + \{\, f \,\}^S$. Now, $x^q u \equiv -xu^q \pmod{W_1}$, so $g \equiv x(y^{q-1}u+u^q) \pmod{W_1}$ and thus $x(y^{q-1}u+u^q) \in W_1+\{\, f \,\}^S$. Apply the endomorphism of $k[x,y]_0$ that is determined by sending $x$ to $y^{q^2-1}$ while fixing $y$ to obtain that $y^{q^2-1}(y^{q-1}u+u^q) \in W_1+\{\, f \,\}^S$. By Lemma 2.1, $y^{q^2-1}(y^{q-1}u+u^q) \equiv y^{q-1}u+u^q \pmod{U_1}$, and so $y^{q-1}u+u^q \in W_1+\{\, f \,\}^S$. Thus the $T$-ideal $\{\, y^{q-1}u+u^q \,\}^T$ is contained in $W_1+\{\, f \,\}^S$. Let $U = U_1 + \{\, y^{q-1}u+u^q \,\}^T$. Then $U_1 \subseteq U \subseteq W_1+\{\, f \,\}^S$. We claim that if $y^{q-1}u+u^q \in W_1$, then $W_1+\{\, f \,\} = k[x,y]_0$. For suppose that $y^{q-1}u+u^q \in W_1$. Since $u^q \equiv -u \pmod{W_1}$, we would then have $y^{q-1}u-u \in W_1$; that is, $\sum_{2\le t<(q+2)/2} \alpha_t((1-t)y^{(t)(q-1)} + (1-t)y^{(t-1)(q-1)}) \in W_1$. Set $m = \lceil \frac{q+2}{2} \rceil - 1$, and observe that $t<(q+2)/2$ means $t\le m$. We would then have

$$-\alpha_2 y^{q-1} + \alpha_m(1-m)y^{m(q-1)} + \sum_{2\le t<m} ((1-t)\alpha_t - t\alpha_{t+1})y^{t(q-1)} \in W_1.$$

Apply the endomorphism of $k[x,y]_0$ that is determined by sending $y$ to $x$ while fixing $x$ to obtain that

$$-\alpha_2 x^{q-1} + \alpha_m(1-m)x^{m(q-1)} + \sum_{2\le t<m} ((1-t)\alpha_t - t\alpha_{t+1})x^{t(q-1)} \in W_1.$$

Note that $t(q-1) = (t-1)q + q - t$ and $q - t > t - 1$ if and only if $q + 1 > 2t$; that is, if and only if $t < m$. Since this condition holds in the above summation, $x^{t(q-1)} \in B_1$ for every $t$ with $2 \le t < m$, as is $x^{q-1}$. If $p$ is odd, then $m = (q+1)/2$, and then $m(q-1)/2 = (q+1)(q-1)/2$. As $(q-1)/2$ would then be a positive integer, we would have $y^{m(q-1)} \in W_1$. If $p$ is even, then $m = q/2$ and $y^{m(q-1)} \in B_1$. Thus $\alpha_2 = 0$, and for each $t$ with $2 \le t \le m-1$, $(1-t)\alpha_t - t\alpha_{t+1} = 0$, so $\alpha_t = 0$ for each $t$ with $2 \le t \le m$. But then $f = \alpha_0 x$, and since $f \neq 0$, we obtain $x \in W_1 + \{\, f \,\}^S$, as claimed.

It remains to consider the case when $y^{q-1}u + u^q \notin W_1$. In this case, $U_1 \subsetneq U \subseteq W_1 + \{\, f \,\}^S$. Suppose that $x \notin W_1 + \{\, f \,\}^S$. Then $U \neq k[x]_0$. Since $U_1$ is precomplete, $U$ is also precomplete, and so by Theorem 8 of [5], $U = \{\, x - x^{q^d} \,\}^T$ for some positive integer $d$. But $U_1 = \{\, x - x^{q^2} \,\}^T \subsetneq U$, so we must have $d = 1$. But then $U = \{\, x - x^q \,\}^T$, the unique maximal (actually, maximum) $T$-space of $k[x,y]_0$, which was shown in [1] also to be a maximal $T$-space. Thus either $W_1 + \{\, f \,\}^S = k[x,y]_0$, or else $W_1 + \{\, f \,\}^S$ is a $T$-ideal. Suppose that $W_1 + \{\, f \,\}^S \neq k[x,y]_0$, so that $W_1 + \{\, f \,\}^S$ is a $T$-ideal of $k[x,y]_0$. Then $x^{q+1}x^i \in W_1 + \{\, f \,\}^S$ for every positive integer $i$. In particular, $x^{q^2} \in W_1 + \{\, f \,\}^S$. But $x \equiv x^{q^2} \pmod{U_1}$ and thus modulo $W_1$, which means that $x \in W_1 + \{\, f \,\}^S$. As this contradicts our assumption that $W_1 + \{\, f \,\}^S \neq k[x,y]_0$, it follows that $W_1 + \{\, f \,\}^S = k[x,y]_0$, as required. ☐

**Proposition 4.3.** *Let $2 \le r \le q-1$. Then for any nonzero $f \in x^{[r]} \cap Y_1$, $W_1 + \{\, f \,\}^S = k[x]_0$.*

*Proof.* We shall prove this by induction on $r$, with the base case provided by Lemma 4.3. Suppose that $r \ge 2$, and that the result holds for all smaller integers. Let $f \in x^{[r]} \cap Y_1$ with $f \neq 0$. By Lemma 4.2, we may assume that

$$f = \sum_{\substack{0 \le t < r/2 \text{ or} \\ r+1 \le t < (q+r+1)/2}} \alpha_t x^{r+t(q-1)}.$$

Note that if $r = q-1$, then there are no indices $t$ for which $r+1 \le t < (q+r+1)/2$.

By Corollary 4.1, it suffices to prove that $W_1 + \{\, f \,\}^S = k[x,y]_0$. In $k[x,y]_0$, let $g$ denote the $q$-homogeneous component of $x^{r-1}y$ in $f(x+y)$. Then

$$g = \sum_{\substack{0 \le t < r/2 \text{ or} \\ r+1 \le t < (q+r+1)/2}} \alpha_t \sum_{0 \le j \le t} \binom{r + t(q-1)}{r - 1 + j(q-1)} x^{r-1+j(q-1)} y^{1+(t-j)(q-1)}.$$

For convenience, let $l = \left\lceil \frac{r}{2} \right\rceil - 1$, so that $t < r/2$ if and only if $t \le l$. Then by Corollary 4.3, (iii) for $t < r/2$ and (iv) for $r + 1 \le t < (q + r + 1)/2$, we find

that

$$g = r\alpha_0 x^{r-1} + \sum_{1\le t\le l} \alpha_t\Big(tx^{r-1+(t-1)(q-1)}y^q + (r-t)x^{r-1+t(q-1)}y\Big)$$
$$+ \sum_{r+1\le t<(q+r+1)/2} \alpha_t \sum_{0\le j\le r-1} \binom{t-1}{j}\binom{q+r-t}{r-1-j} x^{r-1+j(q-1)}y^{1+(t-j)(q-1)}$$
$$+ \sum_{r+1\le t<(q+r+1)/2} \alpha_t\Big((t-1)x^{r-1+(t-1)(q-1)}y^q + (r-t)x^{r-1+t(q-1)}y\Big).$$

We now apply to $g$ the endomorphism of $k[x,y]_0$ that is determined by sending $y$ to $x^{q^2-1}$ while fixing $x$. By Lemma 2.1, the result is congruent modulo $U_1$ to the element that is obtained by deleting $x^{q^2-1}$, which we shall denote by $h$. Thus, after regrouping the terms in the first summation, we find that

$$h = (r-l)\alpha_l x^{r-1+l(q-1)} + \sum_{0\le t\le l-1}\Big((r-t)\alpha_t + (t+1)\alpha_{t+1}\Big)x^{r-1+t(q-1)}$$
$$+ \sum_{r+1\le t<(q+r+1)/2} \alpha_t \sum_{0\le j\le r-1} \binom{t-1}{j}\binom{q+r-t}{r-1-j} x^{r-1+j(q-1)}$$
$$+ \sum_{r+1\le t<(q+r+1)/2} \alpha_t\Big((t-1)x^{r-1+(t-1)(q-1)} + (r-t)x^{r-1+t(q-1)}\Big).$$

Furthermore, since $g \in W_1 + \{\, f\,\}^S$, it follows that $h \in W_1 + \{\, f\,\}^S$ as well. In the first summation above, we note that $t \le l$ if and only if $t \le (r-1)/2$. If $l = (r-1)/2$ (possible of course only if $r$ is odd), then $x^{r-1+l(q-1)} = (x^{q+1})^{(r-1)/2} \in W_1$, and otherwise, $t \le l < (r-1)/2$ has $r-1+t(q-1) = tq+r-1-t$ with $0 \le t < r-1-t < q$, so $x^{r-1+t(q-1)} \in B_1$. A related observation can be made for the second summation displayed above. For $0 \le j \le r-1$, we find that $r-1+j(q-1) = jq+r-1-j$ with $0 \le j, r-1-j < q$, so $x^{r-1+j(q-1)} \in B_1$ if and only if $r-1-j > j$; that is, if and only if $j < (r-1)/2$. Observe that if $j = (r-1)/2$ (possible only when $r$ is odd of course), then $r-1+j(q-1) = (q+1)(r-1)/2$ and so in this case, $x^{r-1+j(q-1)} \in W_1$. Thus in the second summation above, we may exclude the value $j = (r-1)/2$. When $(r-1)/2 < j \le r-1$, then $x^{r-1+j(q-1)} = x^{jq+r-1-j} \equiv -x^{(r-1-j)q+j} = -x^{r-1+(r-j-1)(q-1)} \pmod{W_1}$, and $(r-1)/2 = r-1-(r-1)/2 > r-1-j \ge 0$. Thus, modulo $W_1$,

$$h \equiv (r-l)\alpha_l x^{r-1+l(q-1)} + \sum_{0\le t\le l-1}\Big((r-t)\alpha_t + (t+1)\alpha_{t+1}\Big)x^{r-1+t(q-1)}$$
$$+ \sum_{r+1\le t<(q+r+1)/2} \alpha_t \sum_{0\le j\le l-1} \left(\tbinom{t-1}{j}\tbinom{q+r-t}{r-1-j} - \tbinom{t-1}{r-1-j}\tbinom{q+r-t}{j}\right) x^{r-1+j(q-1)}$$
$$+ \sum_{r+1\le t<(q+r+1)/2} \alpha_t\Big((t-1)x^{r-1+(t-1)(q-1)} + (r-t)x^{r-1+t(q-1)}\Big).$$

For each $t$ with $r+1 \le t < (q+r+1)/2$, and each $j$ with $0 \le j \le l-1$, let $\beta_{t,j} = \binom{t-1}{j}\binom{q+r-t}{r-1-j} - \binom{t-1}{r-1-j}\binom{q+r-t}{j}$, and set

$$h_1 = (r-l)\alpha_l x^{r-1+l(q-1)} + \sum_{0 \le t \le l-1} \Big( (r-t)\alpha_t + (t+1)\alpha_{t+1} \Big) x^{r-1+t(q-1)} + \sum_{r+1 \le t < (q+r+1)/2} \alpha_t \sum_{0 \le j < (r-1)/2} \beta_{t,j} x^{r-1+j(q-1)}$$

and

$$h_2 = \sum_{r+1 \le t < (q+r+1)/2} \alpha_t \Big( (t-1)x^{r-1+(t-1)(q-1)} + (r-t)x^{r-1+t(q-1)} \Big),$$

so $h_1 + h_2 \equiv h \pmod{W_1}$ and thus $h_1 + h_2 \in W_1 + \{ f \}^S$. Furthermore, we have established that if $l < (r-1)/2$, then $h_1$ is in the linear span of $\{ u \in B_1 \mid u = x^{r-1+t(q-1)},\ 0 \le t < (r-1)/2 \}$, while if $l = (r-1)/2$, then $(r-l)\alpha_l x^{r-1+l(q-1)} \in W_1$ and $h_1 - (r-l)\alpha_l x^{r-1+l(q-1)}$ is in the linear span of $\{ u \in B_1 \mid u = x^{r-1+t(q-1)},\ 0 \le t < (r-1)/2 \}$. As for $h_2$, note that for $r+1 \le t < (q+r+1)/2$, we have $q+r > 2t$ and so $q+r-t-1 > t-1$. Thus $r-1+t(q-1) = (t-1)q + (q+r-1-t)$, with $0 < r \le t-1 < q+r-t-1 = q-1-(t-r) < q-1$ and so $x^{r-1+t(q-1)} \in B_1$ for each $t$ with $r+1 \le t < (q+r+1)/2$. Thus $h_2$ is in the linear span of $\{ u \in B_1 \mid u = x^{r-1+t(q-1)},\ r \le t < (q+r+1)/2 \}$. Since these two subsets of $B_1$ are disjoint, it follows that if either $h_1 \notin W_1$ or $h_2 \ne 0$, then $h \equiv h_1 + h_2 \pmod{W_1}$ means that $h \ne 0$ and so $h$ is a nonzero element of $x^{[r-1]} \cap V_1$. But then by the inductive hypothesis, $W_1 + \{ h \}^S = k[x]_0$, and since $h \in W_1 + \{ f \}^S$, it follows that $W_1 + \{ f \}^S = k[x]_0$.

It remains to consider the situation when $h_2 = 0$ and $h_1 \in W_1$; that is, either $r$ is even, so $l < (r-1)/2$ and $h_1 = 0$, or $r$ is odd, so $l = (r-1)/2$ and $h_1 - (r-l)\alpha_l x^{r-1+l(q-1)} = 0$. For this discussion, let $m = \lceil \frac{q+r+1}{2} \rceil - 1$, so $r+1 \le t \le m$. Then we have

$$\begin{aligned} 0 = h_2 &= \sum_{r+1 \le t \le m} \alpha_t \Big( (t-1)x^{r-1+(t-1)(q-1)} + (r-t)x^{r-1+t(q-1)} \Big) \\ &= r\alpha_{r+1} x^{r-1+r(q-1)} + (r-m)\alpha_m x^{r-1+m(q-1)} \\ &\qquad + \sum_{r+1 \le t \le m-1} \Big( \alpha_t(r-t) + \alpha_{t+1} t \Big) x^{r-1+t(q-1)} \end{aligned}$$

As $x^{r-1+t(q-1)} \in B_1$ for each $t$ with $r+1 \le t < (q+r+1)/2$, it follows that $r\alpha_{r+1} = 0$, $(r-m)\alpha_m = 0$, and for each $t$ with $r+1 \le t \le m-1$, we have $\alpha_t(r-t) + \alpha_{t+1} t = 0$. Since neither $t \equiv 0 \pmod{p}$ nor $r - t \equiv 0 \pmod{p}$ for these values of $t$, it follows that $\alpha_t = 0$ for each $t$ with $r+1 \le t < (q+r+1)/2$. We shall take advantage of this information to dramatically simplify the presentation of

$h_1$. Let $l = \lceil \frac{r-1}{2} \rceil - 1$. Then

$$h_1 = (r-l)\alpha_l x^{r-1+l(q-1)} + \sum_{0\le t\le l-1} \Big((r-t)\alpha_t + (t+1)\alpha_{t+1}\Big) x^{r-1+t(q-1)}$$

and so $(r-t)\alpha_t + (t+1)\alpha_{t+1} = 0$ for $0 \le t \le l$. Since neither $r - t \equiv 0 \pmod p$ nor $t + 1 \equiv 0 \pmod p$ for any $t$ under consideration, we have $\alpha_{t+1} = -\frac{(r-t)}{(t+1)}\alpha_t$ for each $t$ with $0 \le t \le l-1$. If $r$ is even, then $l < (r-1)/2$ and then we also have $\alpha_l = 0$, which then implies that $\alpha_t = 0$ for every $t$. Since this would imply that $f = 0$, we may conclude that $r$ is odd, and $l = (r-1)/2$. From the fact that $\alpha_{t+1} = -\frac{(r-t)}{(t+1)}\alpha_t$ for each $t$ with $0 \le t \le l-1$, we find that $\alpha_t = (-1)^t\binom{r}{t}\alpha_0$ for each $t$ with $0 \le t \le (r-1)/2$, and so without loss of generality, we may assume that

$$f = \sum_{0\le t\le (r-1)/2} (-1)^t \binom{r}{t} x^{r+t(q-1)}.$$

We shall not make use of the fact, but it may intrigue the reader to note that for $(r+1)/2 \le t \le r$, we have $r + t(q-1) = (t-1)q + q + r - t$ and $0 \le t-1, r-t$, so $x^{r+t(q-1)} \equiv -x^{(q+r-t)q+t-1} \pmod{W_1}$, and $-x^{(q+r-t)q+t-1} = -x^{q^2+(r-t)q+t-1} \equiv -x^{1+(r-t)q+t-1} = -x^{(r-t)q+t} \pmod{U_1}$. As $-x^{(r-t)q+t} = -x^{(r-t)q+t-r+r} = -x^{r+(r-t)(q-1)}$, and so

$$(-1)^t\binom{r}{t} x^{r+t(q-1)} \equiv (-1)^{t+1}\binom{r}{r-t} x^{r+(r-t)(q-1)} \pmod{W_1}.$$

Since $(-1)^{t+1} = (-1)^{r-t}$, it follows that

$$\sum_{0\le t\le r} (-1)^t\binom{r}{t} x^{r+t(q-1)} \equiv 2 \sum_{0\le t\le (r-1)/2} (-1)^t\binom{r}{t} x^{r+t(q-1)} = 2f \pmod{W_1}.$$

Thus $2f \equiv (x - x^q)^r \pmod{W_1}$, and so if $p > 2$, $f \equiv \frac{1}{2}(x-x^q)^r \pmod{W_1}$.

We now return to our study of $W_1 + \{\, f \,\}^S$. Our work above, when specialized to the current $f$, shows that $g$, the $q$-homogeneous component of $x^{r-1}y$ in $f(x+y)$, is given by

$$g = rx^{r-1}y \quad + \sum_{1\le t\le (r-1)/2} (-1)^t\binom{r}{t}\Big(tx^{r-1+(t-1)(q-1)}y^q + (r-t)x^{r-1+t(q-1)}y\Big),$$

and we know that $g \in W_1 + \{\, f \,\}^S$. Recall that for any $u, v \in k[x,y]_0$, $uv^q \equiv -u^q v \pmod{W_1}$, so $g$ is congruent modulo $W_1$ to

$$rx^{r-1}y \quad + \sum_{1\le t\le (r-1)/2} (-1)^t\binom{r}{t}\Big((-t)x^{q(r-1+(t-1)(q-1))}y + (r-t)x^{r-1+t(q-1)}y\Big),$$

so this element belongs to $W_1 + \{ f \}^S$. Recall also that $U_1 = \{ x - x^{q^2} \}^T \subseteq W_1$, so we obtain that, modulo $U_1$,

$$\begin{aligned} rx^{r-1}y &+ \sum_{1\le t\le (r-1)/2} (-1)^t \binom{r}{t} \Big( (-t)x^{q(r-t)+(t-1)q^2} y + (r-t)x^{r-1+t(q-1)} y \Big) \\ &\equiv y\Big( rx^{r-1} + \sum_{1\le t\le (r-1)/2} (-1)^t \binom{r}{t} \big( (-t)x^{q(r-t)+(t-1)} + (r-t)x^{r-1+t(q-1)} \big) \Big), \end{aligned}$$

and thus

$$y\Big( rx^{r-1} + \sum_{1\le t\le (r-1)/2} (-1)^t \binom{r}{t} \big( (-t)x^{q(r-t)+(t-1)} + (r-t)x^{r-1+t(q-1)} \big) \Big)$$

belongs to $W_1 + \{ f \}^S$. Apply the endomorphism of $k[x,y]_0$ that is determined by sending $y$ to $x^{q^2-1}$ while fixing $x$ to this element, and then apply Lemma 2.1 to obtain that

$$h = rx^{r-1} + \sum_{1\le t\le (r-1)/2} (-1)^t \binom{r}{t} \big( (-t)x^{q(r-t)+(t-1)} + (r-t)x^{r-1+t(q-1)} \big) \Big)$$

belongs to $W_1 + \{ f \}^S$. Observe that

$$\begin{aligned} h &= rx^{r-1} + \sum_{1\le t\le (r-1)/2} (-1)^t \binom{r}{t} \big( (-t)x^{q(r-t)+(t-1)} + (r-t)x^{r-1+t(q-1)} \big) \\ &= rx^{r-1} + rx^{q(r-1)} + \sum_{2\le t\le (r-1)/2} (-1)^t \binom{r}{t} (-t)x^{q(r-t)+(t-1)} \\ &\qquad + \sum_{1\le t\le (r-3)/2} (-1)^t \binom{r}{t} (r-t)x^{r-1+t(q-1)} \\ &\qquad\quad + (-1)^{(r-1)/2} \binom{r}{(r-1)/2} \frac{r-1}{2} (x^{q+1})^{(r-1)/2}. \end{aligned}$$

Now,

$$\sum_{2\le t\le (r-1)/2} (-1)^t \tbinom{r}{t} (-t)x^{q(r-t)+(t-1)} = \sum_{1\le t\le (r-3)/2} (-1)^{t+1} \tbinom{r}{t+1} (-1)(t+1)x^{q(r-t-1)+t}.$$

As well,

$$(-1)^{t+1}\tbinom{r}{t+1}(-1)(t+1) = (-1)^t r!/(t!(r-t-1)!) = (-1)^t \tbinom{r}{t}(r-t).$$

Thus with

$$\beta = (-1)^{(r-1)/2} \tbinom{r}{(r-1)/2} (r-1)/2 \not\equiv 0 \pmod{p},$$

we have

$$h = rx^{r-1} + rx^{q(r-1)} + \sum_{1\le t\le (r-3)/2} (-1)^t \binom{r}{t}(r-t)(x^{q(r-t-1)+t} + x^{tq+r-1-t}) + \beta(x^{q+1})^{(r-1)/2}$$

$$= \sum_{0\le t\le (r-3)/2} (-1)^t \binom{r}{t}(r-t)(x^{q(r-t-1)+t} + x^{q(t)+(r-t-1)}) + \beta(x^{q+1})^{(r-1)/2}.$$

Now, $0 \le t \le (r-1)/2 \le (q-3)/2$ means that $q > q-3 \ge r-t-1 \ge (r-1)/2 \ge t \ge 0$ and $r-t-1+t = r-1 > 0$, so $h$ is in the linear span of $\{ x^{qi+j} + x^{i+qj} \mid q > i \ge j \ge 0,\ i+j > 0 \}$, and since $h \neq 0$, it follows that $h \in W_1 - U_1$. As well, we have $yh \in W_1 + \{ f \}^S$, so $\{ h \}^T \subseteq W_1 + \{ f \}^S$, and $h \notin U_1$ means that $U_1 \subsetneq U = U_1 + \{ h \}^T \subseteq W_1 + \{ f \}^S$. As in the proof of Lemma 4.3, this implies that $U = \{ x - x^q \}^T$ and $W_1 + \{ f \}^S = k[x,y]_0$, as required. This completes the proof of the inductive step, and so the result follows. □

**Theorem 4.1.** *$W_1$ is a maximal $T$-space of $k[x]_0$.*

*Proof.* We must prove that for any $f \in k[x]_0 - W_1$, $W_1 + \{ f \}^S = k[x]_0$. As observed in the discussion following Definition 3.1, it suffices to prove this for each $q$-homogeneous $f \in Y_1$, the linear span of $B_1$. But each $q$-homogeneous element of $Y_1$ is in the class of $x^{[r]}$ for some $r$ with $1 \le r \le q-1$. The result follows now from Lemma 4.3 for $r = 1$, and from Proposition 4.3 for $2 \le r \le q-1$. □

# 5 Summary

We have shown that for any prime $p$, and any finite field $k$ of characteristic $p$ and order $q$, the $T$-spaces $W_{2^n} = \{ x + x^{q^{2^n}}, x^{q^{2^n}+1} \}^S$, $n \ge 0$ are proper, and for any $0 \le m < n$, $W_{2^m} + W_{2^n} = k[x]_0$. We have also proven that $W_1$ is maximal. In [1], for $p > 2$, we had proven that the $T$-spaces $\{ x + x^{q^{2^n}} \}^S$, $n \ge 0$, were proper and had the property that for any $0 \le m < n$, $\{ x + x^{q^{2^m}} \}^S + \{ x + x^{q^{2^n}} \}^S = k[x]_0$, and so were able to conclude that $k[x]_0$ had infinitely many maximal $T$-spaces. From our knowledge of the $k$-linear basis for $W_{2^n}$ that we have obtained in this paper, it follows that $x^{q^{2^n}+1} \notin \{ x + x^{q^{2^n}} \}^S$, so none of the $T$-spaces $\{ x + x^{q^{2^n}} \}^S$ are maximal in $k[x]_0$. For $p = 2$, the situation is somewhat different. Also in [1], we had proven that for $p = 2$, the family of $T$-spaces $\{ x + x^q, x^{q^{2^n}+1} \}^S$, $n \ge 0$, were proper and had the property that the sum of any two is $k[x]_0$. But for $p = 2$, we have $W_{2^n} = \{ x + x^{q^{2^n}}, x^{q^{2^n}+1} \}^S \subseteq \{ x + x^q, x^{q^{2^n}+1} \}^S$, and also from our knowledge of a basis for $W_{2^n}$, we may observe that $x + x^q \notin W_{2^n}$ for $n > 0$. For $n = 0$, the two $T$-spaces coincide, and we have proven that $W_{2^0}$ is a maximal $T$-space of $k[x]_0$. It seems possible that for $p > 2$, $W_{2^n}$ is a maximal

$T$-space of $k[x]_0$ for every $n \geq 0$, and for $p = 2$, $\{\, x + x^q, x^{q^{2^n}+1} \,\}^S$ is a maximal $T$-space of $k[x]_0$ for each $n \geq 0$.

## References


[1] C. Bekh-Ochir and S. A. Rankin, S. A., *Maximal $T$-spaces of a free associative algebra*, J. Algebra, 332 (2011), 442–456.

[2] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly 54 (1947), 589–592.

[3] A. V. Grishin, *On the finite-basis property of systems of generalized polynomials*, Izv. Math. USSR, **37**, no. 2, 1991, 243–272.

[4] A. V. Grishin, *On the finite-basis property of abstract $T$-spaces*, Fund. Prikl. Mat., **1**, 1995, 669–700 (Russian).

[5] T. R. Sundararaman, *Precomplete varieties of $R$-algebras*, Algebra Universalis 3 (1975), 397–405.